REMARKS

Claims 1-8 are pending in the above-identified patent application. Claims 1 and 2 have been amended by way of the present amendment.

In the outstanding Office Action, claims 1 and 2 were objected to due to informalities; and claims 1-8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,016,350 (Funabe et al.) in view of U.S. Publication No. 2002/0073212A1 (Sokol et al.). Reconsideration is respectfully requested.

Claim Objections

Claims 1 and 2 were objected to due to informalities. Claims 1 and 2 have been amended to remove the indicated informalities as suggested in the outstanding Office Action. Therefore, it is respectfully submitted that the rejection of claims 1 and 2 be withdrawn.

35 U.S.C. § 103(a) Claim Rejections

Claims 1-8 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Funabe et al.) in view of Sokol et al. Reconsideration is respectfully requested.

Claim 1, as discussed above, has been amended to recite:

> [a]n encryption apparatus, comprising: a plurality of ports to at least one of which a terminal having an encrypting capability can be directly or indirectly connected; encryption/decryption means for performing an encrypting process and a decrypting process on data to terminate encryption-based security between the terminal having the encrypting capability and/or the non-encrypting capability; and bridge means for allowing data, which has been received with one of the plurality of ports and then on which the encrypting or decrypting process has been performed, to be outputted as it is from another port without being performed any routing process.

Support for the amendments to the claims is provided by the original claims and specification.

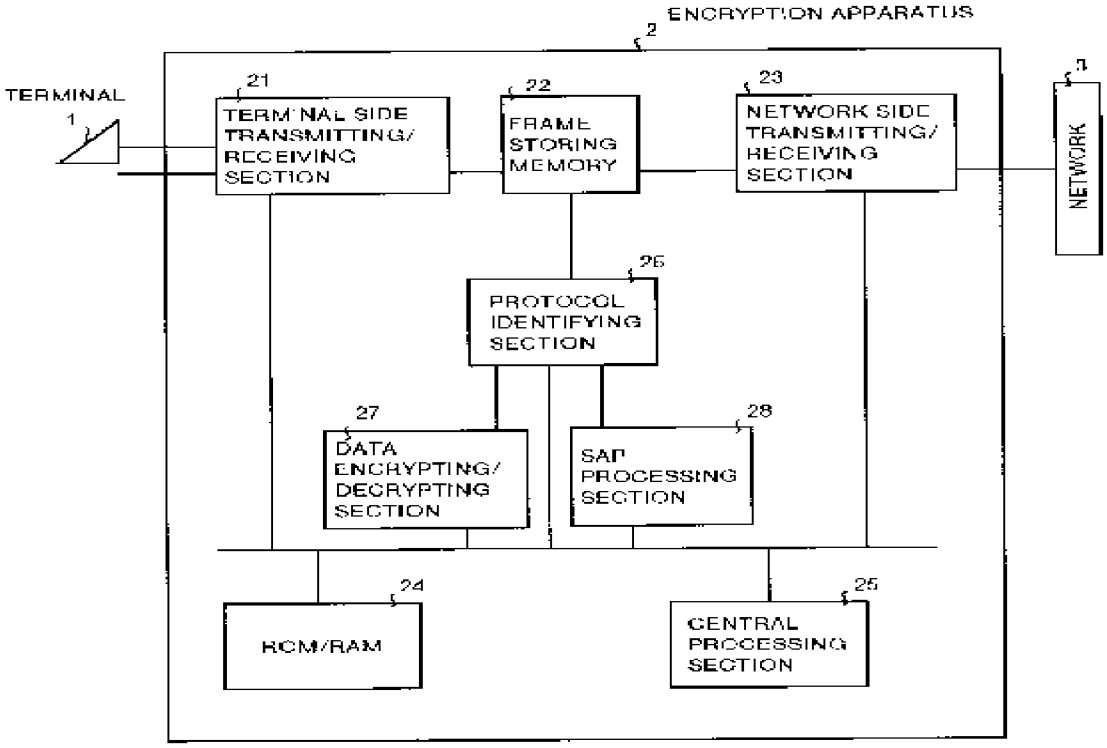
Funabe et al. discloses an encryption apparatus enables encrypted communications using existing network equipment which does not have an encryption function, such as a server, a client, or a router.[1] In particular, as shown in **FIG. 1** below, Funabe et al. discloses a terminal **1**, an encryption apparatus **2**, a network **3**; a terminal side transmitting/receiving section **21** with one or more ports for executing data transaction between the terminal connected to the port and the apparatus; a network side transmitting/receiving section **23** for executing data transaction between a network and the apparatus; a frame storing memory for storing a received frame **22**, a ROM/RAM **24** for storing the program as well as for providing working memory; a central processing section **25** for performing various types of computation; a protocol identifying section **26** for identifying a protocol of the received data; a data encrypting/decrypting section **27** for encrypting/decrypting the received data; an SAP processing section **28** for changing a service type from an non-encryption service to an encryption service if the type is an SAP frame from a terminal, and changing the service type from an encryption service to an non-encryption service if the type is an SAP frame from a network.[2]

Further, Funabe et al. discloses the terminal side transmitting/receiving section **21** in the encryption apparatus stores the received frame in the frame storing memory **22**; the network side transmitting/receiving section **23** stores the received frame in the frame storing memory **22**; and the protocol identifying section **26** identifies a frame protocol, sends the frame if it is an RIP frame, and transfers the frame to the SAP processing section **28** if it is an SAP frame.[3] Furthermore, Funabe et al. discloses the SAP processing section **28** converts a service type 0x04 (non-encryption service), when receiving an SAP frame from the terminal **1**, for instance, to a service type Oxabc (encryption service) for sending to the network **3** through the network side transmitting/receiving section **23**; converts the service type Oxabc, when receiving an SAP frame from the network **3**, to a service type, sets the number of Hops to 0x10 when it is a service type

[1] Funabe et al. at ABSTRACT.
[2] *Id.* at **FIG. 1**; column 6, lines 37 – 60,
[3] *Id.* at **FIG. 1**; column 6, line 61; to column 7, lines 3.

0x04 for sending to the terminal side **1** through the terminal side transmitting/receiving section **21**.[4]

FIG.1



However, Funabe et al. nowhere discloses, as claim 1 recites:

> [a]n encryption apparatus, comprising:
> a plurality of ports to at least one of which a terminal having an encrypting capability can be directly or indirectly connected;

[4] *Id.* at **FIG. 1**; column 7, lines 4-13.

> encryption/decryption means for performing an encrypting process and a decrypting process on data *to terminate encryption-based security between the terminal having the encrypting capability and/or the non-encrypting capability*; and
>
> bridge means for allowing data, which has been received with one of the plurality of ports and then on which the encrypting or decrypting process has been performed, *to be outputted as it is from another port without being performed any routing process* (emphasis added).

That is, the encryption device of claimed invention is a relay device that has a "bridge means" that transmits data without routing and a function to: "terminate encryption-based security between the terminal having the encrypting capability and/or the non-encrypting capability," as recited in claim 1. Further, though Funabe et al. discloses a router having a function to terminate encryption, Funabe et al. does *not disclose a* function for the data to: "be outputted as it is from another port *without being performed any routing process*," as recited in independent claim 1 (emphasis added). Furthermore, similar to the above-emphasized limitation of claim 1,

independent claim 3 recites:

> passing the encrypted or decrypted data to the data link layer and the physical layer *without passing said data to a network layer in which routing between networks is controlled*, and then sending said data to another port so as to be outputted from said port (emphasis added);

and independent claim 5 recites:

> outputting the encrypted or decrypted data from another port through the data link layer and the physical layer, *without passing said data to a network layer in which routing between networks is controlled*" (emphasis added).

Thus, Funabe et al. does not disclose, suggest or make obvious the invention in independent claims 1, 3 and 5, and claims dependent thereon.

In addition, the outstanding Office Action acknowledges other deficiencies of Funabe et al. and attempts to overcome these deficiencies by combining Sokol et al. with Funabe et al. However, Sokol et al. cannot overcome all of the deficiencies of Funabe et al., as discussed below.

Sokol et al. discloses a system in accordance with the invention provides a wireless LAN having terminals that require virtually no setup or installation by the user.[5] In particular, as shown in **FIG. 2** below, Sokol et al. discloses a smartcard reader **122**; and a hub **120** that includes three additional card slots **124, 126, 128**. One of the card slots is a 4-port USB controller **124**, used to connect various peripherals (e.g., printer **132**, scanner **134**) to the hub **120**.[6] Further, Sokol et al. disclose the other two card slots **126, 128** can be used for various

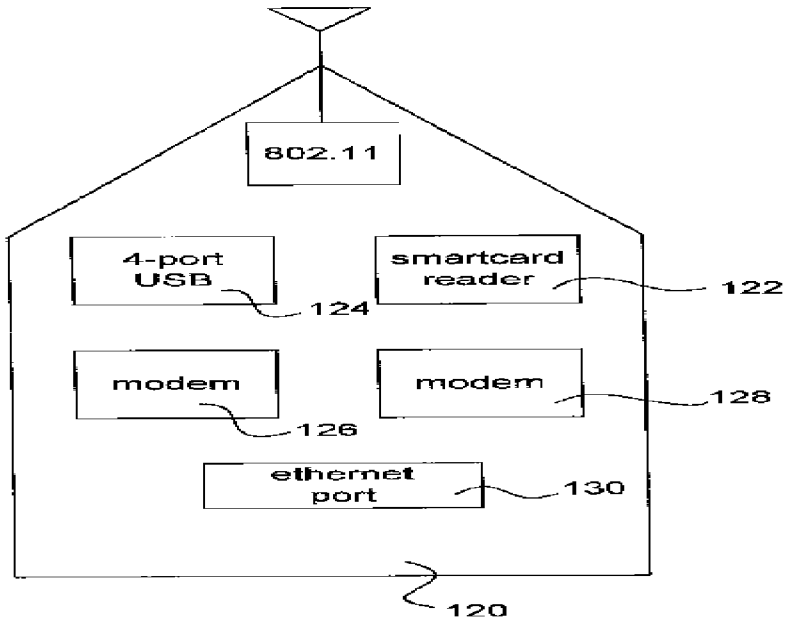


Fig. 2

[5] Sokol et al. at ABSTRACT.
[6] *Id.* at **FIG. 2**; paragraph **[0027]**

devices to form the connection to **ASP 150** and/or the Internet and the hub **120** provides connectivity between a LAN of terminals **102** and an external network served by an **ASP 150**.[7]

Furthermore, Sokol et al. discloses to maintain network security on the wireless network, authentication between the hub and the terminal will be done using wireless equivalent privacy (WEP), or something similar, as is known in the art and that hub **120** connects to the **ASP 150** via a VPN using an open IP Sec Standard in one embodiment.[8]

However, Sokol et al. nowhere discloses, as claim 1 recites:

> [a]n encryption apparatus, comprising:
> a plurality of ports to at least one of which a terminal having an encrypting capability can be directly or indirectly connected;
> encryption/decryption means for performing an encrypting process and a decrypting process on data *to terminate encryption-based security between the terminal having the encrypting capability and/or the non-encrypting capability*; and
> bridge means for allowing data, which has been received with one of the plurality of ports and then on which the encrypting or decrypting process has been performed, *to be outputted as it is from another port without being performed any routing process* (emphasis added).

That is, the encryption device of claimed invention *is a relay device* comprising a function to terminate encryption-based security that has a bridge means to transmit data without routing. In addition, as discussed above, similar to claim 1, independent claims 3 and 5 also recite: "without passing said data to a network layer in which routing between networks is controlled." Thus, in contrast to the claimed invention, Sokol et al. discloses a router of a layer 3 having a function to terminate encryption but *no function to*: "to be outputted as it is from another port without being performed any routing process," as recited in independent claims 1, 3 and 5

[7] *Id.* at **FIG. 2**; paragraph **[0028] to [0029].**
[8] *Id.* at **FIG. 2**; paragraph **[0034]**

In addition, although Sokol et al. discloses a hub that performs no routing, in contrast to the claimed invention discussed above, Sokol et al. is not a relay device, but instead is a line concentrating device that has *no function to*: "terminate encryption-based security between the terminal having the encrypting capability and/or the non-encrypting capability," as recited in the claim 1. Thus, in consideration of the above, Sokol et al. cannot overcome all of the deficiencies of Funabe et al. Therefore, it is respectfully submitted that neither Funabe et al. or Sokol et al., whether taken alone or in combination, does not disclose, suggest or make obvious the claimed invention and that independent claims 1, 3 and 5, and claims dependent thereon, patentably distinguish thereover.

Conclusion

In view of the above, consideration and allowance are respectfully solicited. In the event the Examiner believes an interview might serve in any way to advance the prosecution of this application, the undersigned is available at the telephone number noted below.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 22-0185, under Order No. 22040-00037-US1 from which the undersigned is authorized to draw.

Dated: September 27, 2007

Respectfully submitted,

Electronic signature: /Myron Keith Wyche/
Myron Keith Wyche
Registration No.: 47,341
CONNOLLY BOVE LODGE & HUTZ LLP
1875 Eye Street, NW
Suite 1100
Washington, DC 20006
(202) 331-7111 (Tel)
(202) 293-6229 (Fax)
Agent for Applicant